UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/621,324	07/18/2003	Feihong Chen	129250-000979/US	2523

32498 7590 03/17/2009

CAPITOL PATENT & TRADEMARK LAW FIRM, PLLC
P.O. BOX 1995
VIENNA, VA 22183

EXAMINER	
MOORE, IAN N	

ART UNIT	PAPER NUMBER
2416	

MAIL DATE	DELIVERY MODE
03/17/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/621,324	CHEN ET AL.	
	Examiner	Art Unit	
	IAN N. MOORE	2416	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-13,15-17,19-21 and 23-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2-9,11-13,15-17,19-21,23-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1, 3-5, 7-9, 11-13, 15-17, 19-21, 23-29 have been considered but are moot in view of the new ground(s) of rejection.

Regarding claims 1, 3-5, 7-9, 11-13, 15-17, 19-21, 23-24, the applicant argued that, "…"ingress region"…such definitions are not required in the claim…because the claims and specification clearly define the claimed ingress region and the fault is discussed in Kanakubo falls outside what could reasonably by interpreted as Kanakubo's ingress region, Kanakubo cannot reasonably be relied upon as disclosing the claimed feature of detection a failure along an ingress region of a primary path... examiner interpretation of the term "ingress region" as meaning the region of path between an intermediate router and the destination router is unreasonable, and inconsistent with plain meaning of the words... Kanakubo router LSR-F 3 and LSR-P 1 are two separate and distinct devices…examiner interpretation of phrase "ingress region"....different than (a) a link associated with a source network device, (b) an outgoing link (from the source network device), or (c) a link between the source network device and a neighboring network device… Skalecki does not make up for deficiencies of Kanakubo" on pages 7-8.

In response to applicant's argument, the examiner respectfully disagrees with the argument above.

In response to argument on ""ingress region"…such definitions are not required in the claim", since applicant is <u>not</u> required to recites "the definition" of "ingress region", examiner is

not required to provide any specific meaning of "ingress region". Thus, examiner assertions are reasonable assertion on the broadly claimed invention.

Applicant broadly claimed invention recites "detect a failure along an ingress region of a primary path".

1) Nowhere in the claimed limitation that recites exactly where the failure occurs and what consists of an ingress region. Thus, "in ingress region" can be any where in the network as long as the region is input/incoming region/area/paths of the network. Clearly, Kanakubo FIG. 1 discloses "input/incoming region/area/paths" as set forth in the rejection in the past and this instant rejection.

2) Although applicant does not recite any specific detail "detect a failure along an ingress region of a primary path", applicant repeatedly and incorrectly defining where the failure occurs and exactly what consists of an ingress region in the Kanakubo reference. Thus, the arguments on specific details in Kanakubo based on incorrect assuming is irrelevant and clearly an error.

3) Examiner interpretation is very reasonable since the claim invention is broad. Applicant detailed explanation and interpretation of the "ingress region" is not being claimed in every claim. Examiner can asserts Kanakubo in every part of the broad claimed invention. In fact, one skill in the ordinary art will clearly see that examiner assert the plain meaning of the words and definition of "ingress region" in Kanakubo FIG. 1.

In response to argument on a forwarding table, the claim inventing recites "the device **using** a forwarding table". Thus, the device can use any forwarding table regardless its location. Kanakubo's LSR-P receives fault notification which is used by a forwarding table of LSR-F and LSR-P that included IP and MPLS routing information as set forth below. Thus, it is clear that

the augments based on LSR-F and LSR-P being two different devices is irrelevant and clearly an error.

In response to applicant argument on examiner interpretation, it is noted that none of the independent claim 1, 5, 9, 13, 17 recites "(a) a link associated with a source network device, (b) an outgoing link (from the source network device), or (c) a link between the source network device and a neighboring network device". Thus, the argument on limitations that are not even recited in the claims is irrelevant.

In response to applicant argument, Kanakubo disclose that "ingress region" is

(a) a link associated with source network device (see FIG. 1, input/ingress side/region comprises a link/path (e.g. a link/path between LSR 1, 2, 3,6) associated with LSR-1; see page 2, paragraph 25-30),

(b) the link comprises either an outgoing link (see FIG. 1, a link/path is the transmit/output/outgoing link of Node LSP-1) or

(c) a link between the source network device and a neighboring network device (see FIG. 1, a link/path between LSR-1 and LSR-6; see page 2, paragraph 25-30).

Skalecki teaches a source network device (see FIG. 2-3, Node A) operable to: detecting a failure along in ingress region of a primary path (see FIG. 2-3, detect a fault along in the input/ingress area/region of the working path W1), where the ingress region comprises

(a) a link (see FIG. 2-3, input/ingress area/region comprises a path/link/connection) associated with the source network device (see FIG. 2-3, associated/related with Node A),

(b) the link comprises an outgoing link (see FIG. 2-3, link/path/connection comprising outgoing/transmit link/line/connection) or

(c) a link between the source network device and a neighboring network device (see FIG. 2, 3, link/path/connection between Node A and Node K; see page 3-4, paragraph 34-43).

In view of the above, it is clear that the combined system of Kanakubo and Skalecki clearly discloses the applicant broadly claimed invention, and examiner interpretation is proper.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, the rejection is based combined system, and thus when considering the system as a whole, it is clear that the combined system discloses applicant broadly claimed invention.

Regarding claims 1, 3-5, 7-9, 11-13, 15-17, 19-21, 23-24, the applicant argued that, "…allowing traffic to travel along a primary path when the failure is no longer detected along in ingress region. Dantu is simply not pertinent to this feature…there is no disclosure of a fault along the ingress portion of the ring…there is no disclosure of primary paths as that phrase is used in the specification and claims of the present application… Skalecki…there is no disclosure that the working path is restored for usage after a failure is no longer detected along an ingress region…" in pages 9-10.

In response to applicant's argument, the examiner respectfully disagrees with the argument above.

In response to argument on the usage of phrase "primary path", Dantu discloses "working path" which examiner asserts as "primary path" since they both have identical

functionality of primarily carrying data until failure. Thus, Dantu clearly discloses the argued limitation.

In response to applicant's argument that the references fail to show certain features of applicant's invention **based on specification**, it is noted that none of those specific features relevant to **"ingress region" and primary path"** recited in the specification are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Dantu discloses means for detecting (**see FIG. 4, a combined system of processor 402, memory 404, and interface 412 performing examining/detecting; see col. 9, line 30 to col. 11, line 26; or see FIG. 5, a combined system of processor 502, memory 504, and interface 512 performing examining/detecting; see col. 12, line 39-64; see col. 13, line 30-40**) a failure along an ingress region of a primary path (**see FIG. 3, a failure occurs on a working path 332 between node 344 and 348; see FIG. 9, step 902; see FIG. 10, step 1002; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36**); and

However, switching back from the alternating/protection path to the primary path after the failure is recovered is well known in the art as "revertive" switching or "fail-back" switching as one can evident in view of Skalecki .

In particular, Skalecki teaches a source network device (see FIG. 2-3, Node A) operable to: means for detecting a failure along in ingress region of a primary path (**see FIG. 2-3, detect a fault along in the input/ingress area/region of the working path W1; see page 3-4, paragraph 34-43**); means for re-routing traffic from the primary path to an alternate path (**see**

FIG. 2, 3, switch the traffic form working path W1 to protection path P1; see page 3-4, paragraph 39-48); means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region (**see FIG. 5, Switching Node switches the traffic from protecting path to working path when the restoring path message is received along in the input/ingress area/region of the working path W1; see FIG. 6, S602-608; see page 2, paragraph 20-23; see page 4-5, paragraph 55-59**).

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, the rejection is based combined system, and thus when considering the system as a whole, it is clear that the combined system discloses applicant broadly claimed invention.

Claim Objections

2. Claims 1, 3, 4, 5, 7, 8, 25-29 are objected to because of the following informalities:

Claim 1 recites "a network device" which is an apparatus claim; however, the body of the claim recites the method steps of "detecting…re-routing…allowing…" Thus, for clarity, it is revised the claim such that the claim does not recite the method steps.

Claims 5, 25, and 28 are also objected for the same reason as set forth above in claim 1.

Claims 3, 4, 7, 8, 26, 27, and 29 are also objected since they are depended upon objected claims as set forth above.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21, and 23-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanakubo (US 20030147346A1) in view of Skalecki (US 20040004937).

Regarding Claims 1, 9, and 17, Kanakubo discloses a network device processing a method (see FIG. 1, LSR-P 1) comprising:

means for detecting a failure (see FIG. 2, LSR 1 receiving/detecting fault occurrence a1) along an ingress region of a primary path (see FIG. 1, receiving fault indication along input/ingress side of normal LSP; see page 2, paragraph 25-30); and

means for re-routing traffic (see FIG. 1, LSR-P performing LSP switching) from the primary path associated with an original IP address (see FIG. 1, from a normal path corresponding to protection point IP address) to an alternate path (see FIG. 1, to bypass LSP; see page 2, paragraph 29-36) which includes the device using a forwarding table (see FIG. 3, using LSP fault indication retrieval table) that includes Internet Protocol (IP) (see FIG. 3, IP address of the protection point) and Multi-Protocol Label Switched (MPLS) routing information (see FIG. 3, entry type and entry) while associating the original IP address to the alternate path upon

detection of the failure (see FIG. 3, LSP fault indication retrieval table associates IP address of protection point to the bypass path when receiving fault indication; see page 3, paragraph 39-53).

Kanakubo does not explicitly disclose "means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region".

However, switching back from the alternating/protection path to the primary path after the failure is recovered is well known in the art as "revertive" switching or "fail-back" switching. In particular, Skalecki teaches a source network device (see FIG. 2-3, Node A) operable to:

means for detecting a failure along in ingress region of a primary path (see FIG. 2-3, detect a fault along in the input/ingress area/region of the working path W1; see page 3-4, paragraph 34-43)

means for re-routing traffic from the primary path to an alternate path (see FIG. 2, 3, switch the traffic form working path W1 to protection path P1; see page 3-4, paragraph 39-48);

means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region (**see FIG. 5, Switching Node switches the traffic from protecting path to working path when the restoring path message is received along in the input/ingress area/region of the working path W1; see FIG. 6, S602-608; see page 2, paragraph 20-23; see page 4-5, paragraph 55-59**).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide "means for allowing traffic to travel along the primary path when the failure is no longer detected along in ingress region" as taught by Skalecki in the system of Kanakubo, so that it would provide the efficient use of the network resources; see Skalecki page 1, paragraph 66-67.

Regarding Claims 5, 13 and 21, Kanakubo discloses a network device processing a method (see FIG. 1, LSR-P 1) comprising:

means for receiving a failure message (see FIG. 2, LSR 1 receiving/detecting fault occurrence a1);

means for re-routing traffic, after receiving, (see FIG. 1, LSR-P performing LSP switching) from a primary path associated with an original IP address (see FIG. 1, from a normal LSP path corresponding to protection point IP address; see page 2, paragraph 25-30) to an alternate path (see FIG. 1, to bypass LSP; see page 2, paragraph 29-36) using a forwarding table (see FIG. 3, using LSP fault indication retrieval table) that includes IP see FIG. 3, IP address of the protection point) and MPLS routing information (see FIG. 3, entry type and entry), said means for re-routing maintaining the original address (see FIG. 3, LSP fault indication retrieval table associates IP address of protection point to the bypass path; see page 3, paragraph 39-53), the alternate path comprising devices (see FIG. 1, LSR 4 and LSR 5) which maintain the same quality of service as the primary path (see page 1, paragraph 17; see page 3, paragraph 37, 54; see page 4, paragraph 60; bypass LSP comprising LSR 4 and LSR 5 and bypass LSP utilizes the same QoS policy as normal LSP since it is predefined/static LSP) and are not a part of the primary path except for the network device and a destination network device (see FIG. LSR 4 and 5 are not part of the normal LSP except LSR-P 1 and LSR-6; see page 2, paragraph 25-32).

Kanakubo does not explicitly disclose "allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region".

However, switching back from the alternating/protection path to the primary path after the failure is recovered is well known in the art as “revertive" switching or "fail-back" switching. In particular, Skalecki teaches a network device (see FIG. 2-3, Node A) operable to:

receive a failure message (see FIG. 2-3, receiving link down message I’ indicated of fault; see page 3, paragraph 39-40, 43)

re-routing traffic from the primary path to an alternate path (see FIG. 2, 3, switch the traffic form working path W1 to protection path P1; see page 3-4, paragraph 39-48);

allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region (**see FIG. 5, Switching Node switches the traffic from protecting path to working path when the restoring path message is received along in the input/ingress area/region of the working path W1; see FIG. 6, S602-608; see page 2, paragraph 20-23; see page 4-5, paragraph 55-59**).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide “means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region” as taught by Skalecki in the system of Kanakubo, so that it would provide the efficient use of the network resources; see Skalecki page 1, paragraph 66-67.

Regarding Claims 25, 27 and 28, Kanakubo discloses a network device (see FIG. 1, LSR-P 1) comprising:

detecting a failure (see FIG. 2, LSR 1 receiving/detecting fault occurrence a1) along an ingress region of a primary path (see FIG. 1, receiving fault indication along input/ingress side/region (e.g. a region between LSRs 1, 2, 3, 6) of normal LSP; see page 2, paragraph 25-30),

where the ingress region comprises a link associated with source network device (see FIG. 1, input/ingress side/region comprises a link/path (e.g. a link/path between LSR 1,2,3,6) associated with LSR-1; see page 2, paragraph 25-30), the link comprises either an outgoing link (see FIG. 1, a link/path is the transmit/output/outgoing link of Node LSP-1) or a link between the source network device and a neighboring network device (see FIG. 1, a link/path between LSR-1 and LSR-6; see page 2, paragraph 25-30) and

re-routing traffic (see FIG. 1, LSR-P performing LSP switching) from the primary path associated with an original IP address (see FIG. 1, from a normal path corresponding to protection point IP address) to an alternate path (see FIG. 1, to bypass LSP; see page 2, paragraph 29-36) which includes the device using a forwarding table (see FIG. 3, using LSP fault indication retrieval table) that includes Internet Protocol (IP) (see FIG. 3, IP address of the protection point) and Multi-Protocol Label Switched (MPLS) routing information (see FIG. 3, entry type and entry) while associating the original IP address to the alternate path upon detection of the failure (see FIG. 3, LSP fault indication retrieval table associates IP address of protection point to the bypass path when receiving fault indication; see page 3, paragraph 39-53).

Kanakubo does not explicitly disclose “allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region”.

However, switching back from the alternating/protection path to the primary path after the failure is recovered is well known in the art as “revertive" switching or "fail-back" switching. In particular, Skalecki teaches a source network device (see FIG. 2-3, Node A) operable to:

detecting a failure along in ingress region of a primary path (see FIG. 2-3, detect a fault along in the input/ingress area/region of the working path W1), where the ingress region

comprises a link (see FIG. 2-3, input/ingress area/region comprises a path/link/connection) associated with the source network device (see FIG. 2-3, associated/related with Node A), and the link comprises an outgoing link (see FIG. 2-3, link/path/connection comprising outgoing/transmit link/line/connection) **or** a link between the source network device and a neighboring network device (see FIG. 2, 3, link/path/connection between Node A and Node K; see page 3-4, paragraph 34-43);

re-routing traffic from the primary path to an alternate path (see FIG. 2, 3, switch the traffic form working path W1 to protection path P1; see page 3-4, paragraph 39-48);

allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region (**see FIG. 5, Switching Node switches the traffic from protecting path to working path when the restoring path message is received along in the input/ingress area/region of the working path W1; see FIG. 6, S602-608; see page 2, paragraph 20-23; see page 4-5, paragraph 55-59**).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide "allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region" as taught by Skalecki in the system of Kanakubo, so that it would provide the efficient use of the network resources; see Skalecki page 1, paragraph 66-67.

Regarding Claims 3, 7, 11, 15, 19, 23, 26 and 29, Kanakubo discloses the device is a multi-protocol label switched (MPLS) device (see FIG. 1, MPLS label switch Router (LSR) 1) and the primary and alternate paths are label switched paths (LSPs) (see FIG. 1, normal and bypass Label Switch Paths (LSPs); see page 2, paragraph 25-26).

Regarding Claims 4, 12 and 20, Kanakubo discloses the failure is along a link between the device and the neighboring network device (see FIG. 1, fault occurrence a1 is along the LSP link between LSR-P 1 and LSR 6; see page 2, paragraph 25-29).

Regarding Claims 8, 16, and 24, Kanakubo discloses the quality of service is associated with bandwidth (see page 3, paragraph 37; the basic operation of QoS policy such as Diff-serv (differentiated service) class, band and service. Note in Diff-serv QoS/class policy band is the bandwidth (i.e. transmission data amount per unit time for each band/flow)).

5. Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21, and 23-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dantu (US007167443B1) in view of Skalecki (US 20040004937).

Regarding Claims 1, 9 and 17, Dantu discloses a network device (see FIG. 3, node 300/340/344/348; see FIG. 4-5, node 400/500; or see FIG. 6, Node 600/616/620/624) processing a method (see FIG. 9-11, Method) comprising:

means for detecting (see FIG. 4, a combined system of processor 402, memory 404, and interface 412 performing examining/detecting; see col. 9, line 30 to col. 11, line 26; or see FIG. 5, a combined system of processor 502, memory 504, and interface 512 performing examining/detecting; see col. 12, line 39-64; see col. 13, line 30-40) a failure along an ingress region of a primary path (see FIG. 3, a failure occurs on a working path 332 between node 344 and 348; see FIG. 9, step 902; see FIG. 10, step 1002; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36); and

means for re-routing traffic (see FIG. 4, a combined system of processor 402, memory 404, storage 406 performing switching to protecting path ring in node 400; see col. 9, line 30 to

col. 11, line 26; or see FIG. 5, a combined system of processor 502, memory 504, and storage 506 performing switching to protecting path ring in node 500; see col. 12, line 39-64; see col. 13, line 30-40) from the primary path associated with an original IP address (see FIG. 7, IP address 712/08) to an alternate path (see FIG. 3,6, protection path 336; see FIG. 7, a label 716 with path route) which includes the device using a forwarding table that includes Internet Protocol (IP) and Multi-Protocol Label Switched (MPLS) routing information (see FIG. 3, Forwarding table 312 and/or routing table 308; see FIG. 4, a combined system of memory 404 (e.g. routing table 404 A and forwarding table 404B) and storage 406 (e.g. table formation 406A and protection switching 406B) in node 400 includes IP addresses corresponding to MPLS labels; or see FIG. 5, a combined system of memory 504 (e.g. forwarding table 504A) and storage 506 (e.g. forwarding logic 506) in node 500 includes IP addresses corresponding to MPLS labels; see FIG. 10, S 1004, see FIG. 11, S 1104,1106; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-45) while associating the original IP address to the alternate path upon detection of the failure (see FIG. 4,5; see FIG. 10, S 1006,1008,1010; see FIG. 11, S 1108; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-46; switching IP address with its corresponding new label to the protection path when detecting a failure).

Dantu does not explicitly disclose "means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region".

However, switching back from the alternating/protection path to the primary path after the failure is recovered is well known in the art as “revertive" switching or "fail-back" switching. In particular, Skalecki teaches a source network device (see FIG. 2-3, Node A) operable to:

means for detecting a failure along in ingress region of a primary path (see FIG. 2-3, detect a fault along in the input/ingress area/region of the working path W1; see page 3-4, paragraph 34-43);

means for re-routing traffic from the primary path to an alternate path (see FIG. 2, 3, switch the traffic form working path W1 to protection path P1; see page 3-4, paragraph 39-48);

means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region (**see FIG. 5, Switching Node switches the traffic from protecting path to working path when the restoring path message is received along in the input/ingress area/region of the working path W1; see FIG. 6, S602-608; see page 2, paragraph 20-23; see page 4-5, paragraph 55-59**).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide “means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region” as taught by Skalecki in the system of Dantu, so that it would provide the efficient use of the network resources; see Skalecki page 1, paragraph 66-67.

Regarding Claims 5, 13 and 21, Dantu discloses a network device (see FIG. 3, node 300/340/344/348; see FIG. 4-5, node 400/500; or see FIG. 6, Node 600/616/620/624) processing a method (see FIG. 9-11, Method) comprising:

means for receiving (see FIG. 4, Interface I/F 412; see FIG. 5, Interface I/F 512) a failure message (see FIG. 9, S 906, receiving a signal with error indication; see col. 17, line 11 to col. 18, line 11);

means for re-routing traffic (see FIG. 4, a combined system of processor 402, memory 404, storage 406 performing switching to protecting path ring in node 400; see col. 9, line 30 to col. 11, line 26; or see FIG. 5, a combined system of processor 502, memory 504, and storage 506 performing switching to protecting path ring in node 500; see col. 12, line 39-64; see col. 13, line 30-40) from a primary path (see FIG. 3, a working path 332; see FIG. 9, step 902; see FIG. 10, step 1002; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36) associated with an original IP address (see FIG. 7, IP address 712/08) to an alternate path (see FIG. 3,6, protection path 336; see FIG. 7, a label 716 with path route) using a forwarding table that includes IP and MPLS routing information (see FIG. 3, Forwarding table 312 and/or routing table 308; see FIG. 4, a combined system of memory 404 (e.g. routing table 404 A and forwarding table 404B) and storage 406 (e.g. table formation 406A and protection switching 406B) in node 400 includes IP addresses corresponding to MPLS labels; or see FIG. 5, a combined system of memory 504 (e.g. forwarding table 504A) and storage 506 (e.g. forwarding logic 506) in node 500 includes IP addresses corresponding to MPLS labels; see FIG. 10, S 1004, see FIG. 11, S 1104,1106; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-45), said means for re-routing maintaining the original address (see FIG. 4,5; see FIG. 10, S 1006,1008,1010; see FIG. 11, S 1108; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line

45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-46; switching IP address with its corresponding new label to the protection path), the alternate path comprising devices (see FIG. 3, intermediate nodes 348) which maintain the same quality of service as the primary path (see FIG. 10, S 1106,1008,1010; FIG. 11, S 1104-1108; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-46; assigning QoS level of IP packet in the working path to the same QoS level in the protection path while creating a new label) and are not a part of the primary path except for the network device and a destination network device (see FIG. 3, intermediate node 348 are not part of the working path; see col. 8, line 60 to col. 9, line 62).

Dantu does not explicitly disclose "allow traffic to travel along the primary path when the failure is no longer detected along the ingress region".

However, switching back from the alternating/protection path to the primary path after the failure is recovered is well known in the art as "revertive" switching or "fail-back" switching. In particular, Skalecki teaches a network device (see FIG. 2-3, Node A) operable to:

receive a failure message (see FIG. 2-3, receiving link down message I' indicated of fault; see page 3, paragraph 39-40, 43)

re-routing traffic from the primary path to an alternate path (see FIG. 2, 3, switch the traffic form working path W1 to protection path P1; see page 3-4, paragraph 39-48);

allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region **(see FIG. 5, Switching Node switches the traffic from protecting path to working path when the restoring path message is received along in the**

input/ingress area/region of the working path W1; see FIG. 6, S602-608; see page 2, paragraph 20-23; see page 4-5, paragraph 55-59).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide "means for allowing traffic to travel along the primary path when the failure is no longer detected" as taught by Skalecki in the system of Dantu, so that it would provide the efficient use of the network resources; see Skalecki page 1, paragraph 66-67.

Regarding Claim 25, 27 and 28, Dantu discloses a network device (see FIG. 3, node 300/340/344/348; see FIG. 4-5, node 400/500; or see FIG. 6, Node 600/616/620/624) for:

detecting (see FIG. 4, a combined system of processor 402, memory 404, and interface 412 performing examining/detecting; see col. 9, line 30 to col. 11, line 26; or see FIG. 5, a combined system of processor 502, memory 504, and interface 512 performing examining/detecting; see col. 12, line 39-64; see col. 13, line 30-40) a failure along an ingress region of a primary path (see FIG. 3, a failure along a input/ingress region/section of the working path 332 between node 344 and 348 ; or see FIG. 6, a failure along a input/ingress region/section of the working path between node 600, 616, 620; see FIG. 9, step 902; see FIG. 10, step 1002; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36), where the ingress region comprises a link associated with the source network device (see FIG. 3, input/ingress region/section comprises a path/link 332 associated with the node (e.g. Node 300); or see FIG. 6, input/ingress region/section comprises a path/link associated with the node 600; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36), and the link comprises either an outgoing link (see FIG. 3, a path/link 332 comprising a transmit link/line to Node 340 or 348; or see FIG. 6, a path/link at node 600 comprising a transmit link/line to Node

616, 624; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36;,) **or** a link between the source network device and a neighboring network device (see FIG. 3, a path/link between Node 300 and neighbor node 340/344/348; or see FIG. 3, a path/link between Node 600 and neighbor node 616, 624, 620; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36); and

re-routing traffic (see FIG. 4, a combined system of processor 402, memory 404, storage 406 performing switching to protecting path ring in node 400; see col. 9, line 30 to col. 11, line 26; or see FIG. 5, a combined system of processor 502, memory 504, and storage 506 performing switching to protecting path ring in node 500; see col. 12, line 39-64; see col. 13, line 30-40) from the primary path associated with an original IP address (see FIG. 7, IP address 712/08) to an alternate path (see FIG. 3,6, protection path 336; see FIG. 7, a label 716 with path route) which includes the device using a forwarding table that includes Internet Protocol (IP) and Multi-Protocol Label Switched (MPLS) routing information (see FIG. 3, Forwarding table 312 and/or routing table 308; see FIG. 4, a combined system of memory 404 (e.g. routing table 404 A and forwarding table 404B) and storage 406 (e.g. table formation 406A and protection switching 406B) in node 400 includes IP addresses corresponding to MPLS labels; or see FIG. 5, a combined system of memory 504 (e.g. forwarding table 504A) and storage 506 (e.g. forwarding logic 506) in node 500 includes IP addresses corresponding to MPLS labels; see FIG. 10, S 1004, see FIG. 11, S 1104,1106; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-45) while associating the original IP address to the alternate path upon detection of the failure (see FIG. 4,5; see FIG. 10, S 1006,1008,1010; see FIG. 11, S

1108; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-46; switching IP address with its corresponding new label to the protection path when detecting a failure).

Dantu does not explicitly disclose "allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region".

However, switching back from the alternating/protection path to the primary path after the failure is recovered is well known in the art as "revertive" switching or "fail-back" switching. In particular, Skalecki teaches a source network device (see FIG. 2-3, Node A) for:

detecting a failure along in ingress region of a primary path (see FIG. 2-3, detect a fault along in the input/ingress area/region of the working path W1), where the ingress region comprises a link (see FIG. 2-3, input/ingress area/region comprises a path/link/connection) associated with the source network device (see FIG. 2-3, associated/related with Node A), and the link comprises an outgoing link (see FIG. 2-3, link/path/connection comprising outgoing/transmit link/line/connection) **or** a link between the source network device and a neighboring network device (see FIG. 2, 3, link/path/connection between Node A and Node K; see page 3-4, paragraph 34-43

re-routing traffic from the primary path to an alternate path (see FIG. 2, 3, switch the traffic form working path W1 to protection path P1; see page 3-4, paragraph 39-48);

allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region **(see FIG. 5, Switching Node switches the traffic from protecting path to working path when the restoring path message is received along in the**

input/ingress area/region of the working path W1; see FIG. 6, S602-608; see page 2, paragraph 20-23; see page 4-5, paragraph 55-59).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide "means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region" as taught by Skalecki in the system of Dantu, so that it would provide the efficient use of the network resources; see Skalecki page 1, paragraph 66-67.

Regarding Claims 3,7, 11, 15, 19, 23, 26 and 29, Dantu discloses the device is a multi-protocol label switched (MPLS) device (see FIG. 3, Node 300 with MPSL switching capability; or see FIG. 6, 7, MPLS label switch Node 600; see col. 9, line 30-36; see col. 13, line 30-35; see col. 14, line 50-65; see col. 15, line 45-65) and the primary and alternate paths are label switched paths (LSPs) (see FIG. 1, working and protection paths are label Switch Paths; see col. 9, line 30-36; see col. 13, line 30-35; see col. 14, line 50-65; see col. 15, line 45-65).

Regarding Claims 4, 12 and 20, Dantu discloses the failure is at a neighboring device (see FIG. 3, a failure occurs at neighbor node 344/348; or see FIG. 6, a failure occurs at neighbor node 616,620,622) **or** along a link between the device and the neighboring network device (see FIG. 3, failure occurs between node 300 and node 344; or see FIG. 3, failure occurs between node 600 and node 616/620; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36).

Regarding Claims 8, 16, and 24, Dantu discloses the quality of service is associated with bandwidth (see col. 16, line 1-36; see col. 19, line 35-46; QoS associated with bandwith or throughput or resources).

6. Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21, and 23-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dantu (US007167443B1) in view of Anderson (US 5838924).

Regarding Claims 1, 9 and 17, Dantu discloses a network device (see FIG. 3, node 300/340/344/348; see FIG. 4-5, node 400/500; or see FIG. 6, Node 600/616/620/624) processing a method (see FIG. 9-11, Method) comprising:

means for detecting (see FIG. 4, a combined system of processor 402, memory 404, and interface 412 performing examining/detecting; see col. 9, line 30 to col. 11, line 26; or see FIG. 5, a combined system of processor 502, memory 504, and interface 512 performing examining/detecting; see col. 12, line 39-64; see col. 13, line 30-40) a failure along an ingress region of a primary path (see FIG. 3, a failure occurs on a working path 332 between node 344 and 348; see FIG. 9, step 902; see FIG. 10, step 1002; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36); and

means for re-routing traffic (see FIG. 4, a combined system of processor 402, memory 404, storage 406 performing switching to protecting path ring in node 400; see col. 9, line 30 to col. 11, line 26; or see FIG. 5, a combined system of processor 502, memory 504, and storage 506 performing switching to protecting path ring in node 500; see col. 12, line 39-64; see col. 13, line 30-40) from the primary path associated with an original IP address (see FIG. 7, IP address 712/08) to an alternate path (see FIG. 3,6, protection path 336; see FIG. 7, a label 716 with path route) which includes the device using a forwarding table that includes Internet Protocol (IP) and Multi-Protocol Label Switched (MPLS) routing information (see FIG. 3, Forwarding table 312 and/or routing table 308; see FIG. 4, a combined system of memory 404 (e.g. routing table 404 A

and forwarding table 404B) and storage 406 (e.g. table formation 406A and protection switching 406B) in node 400 includes IP addresses corresponding to MPLS labels; or see FIG. 5, a combined system of memory 504 (e.g. forwarding table 504A) and storage 506 (e.g. forwarding logic 506) in node 500 includes IP addresses corresponding to MPLS labels; see FIG. 10, S 1004, see FIG. 11, S 1104,1106; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-45) while associating the original IP address to the alternate path upon detection of the failure (see FIG. 4,5; see FIG. 10, S 1006,1008,1010; see FIG. 11, S 1108; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-46; switching IP address with its corresponding new label to the protection path when detecting a failure).

Dantu does not explicitly disclose “means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region”.

However, switching back from the alternating/protection path to the primary path after the failure is recovered is well known in the art as “revertive" switching or "fail-back" switching. In particular, Anderson teaches a network device (see FIG. 1-2, Node 103) operable to:

means for detecting a failure along in ingress region of a primary path (see FIG. 2, detect a physical layer defect/failure along in the input/ingress area/region (e.g. between node 101 and 103) of the working VPG; see col. 4, line 15 to col. 5, line 30);

means for re-routing traffic from the primary path to an alternate path (see FIG. 2, 3, switch the traffic from working VPG to protection VPG; see col. 4, line 15 to col. 5, line 30);

means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region (see FIG. 1, Node 103 reverts the traffic from protecting VPG to working VPG when the working VPG defect/failure is cleared along in the input/ingress area/region of the working VPG (e.g. between node 101 and 103); see col. 4, line 50 to col. 5, line 15).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide "means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region" as taught by Anderson in the system of Dantu, so that it would provide extremely fast protection switching of an extremely large number of ATM virtual connections; see Anderson col. 2, line 15-20.

Regarding Claims 5, 13 and 21, Dantu discloses a network device (see FIG. 3, node 300/340/344/348; see FIG. 4-5, node 400/500; or see FIG. 6, Node 600/616/620/624) processing a method (see FIG. 9-11, Method) comprising:

means for receiving (see FIG. 4, Interface I/F 412; see FIG. 5, Interface I/F 512) a failure message (see FIG. 9, S 906, receiving a signal with error indication; see col. 17, line 11 to col. 18, line 11);

means for re-routing traffic (see FIG. 4, a combined system of processor 402, memory 404, storage 406 performing switching to protecting path ring in node 400; see col. 9, line 30 to col. 11, line 26; or see FIG. 5, a combined system of processor 502, memory 504, and storage 506 performing switching to protecting path ring in node 500; see col. 12, line 39-64; see col. 13, line 30-40) from a primary path (see FIG. 3, a working path 332; see FIG. 9, step 902; see FIG. 10, step 1002; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36)

associated with an original IP address (see FIG. 7, IP address 712/08) to an alternate path (see FIG. 3,6, protection path 336; see FIG. 7, a label 716 with path route) using a forwarding table that includes IP and MPLS routing information (see FIG. 3, Forwarding table 312 and/or routing table 308; see FIG. 4, a combined system of memory 404 (e.g. routing table 404 A and forwarding table 404B) and storage 406 (e.g. table formation 406A and protection switching 406B) in node 400 includes IP addresses corresponding to MPLS labels; or see FIG. 5, a combined system of memory 504 (e.g. forwarding table 504A) and storage 506 (e.g. forwarding logic 506) in node 500 includes IP addresses corresponding to MPLS labels; see FIG. 10, S 1004, see FIG. 11, S 1104,1106; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-45), said means for re-routing maintaining the original address (see FIG. 4,5; see FIG. 10, S 1006,1008,1010; see FIG. 11, S 1108; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-46; switching IP address with its corresponding new label to the protection path), the alternate path comprising devices (see FIG. 3, intermediate nodes 348) which maintain the same quality of service as the primary path (see FIG. 10, S 1106,1008,1010; FIG. 11, S 1104-1108; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-46; assigning QoS level of IP packet in the working path to the same QoS level in the protection path while creating a new label) and are not a part of the primary path except for the network device and a

destination network device (see FIG. 3, intermediate node 348 are not part of the working path; see col. 8, line 60 to col. 9, line 62).

Dantu does not explicitly disclose “allow traffic to travel along the primary path when the failure is no longer detected along the ingress region”.

However, switching back from the alternating/protection path to the primary path after the failure is recovered is well known in the art as “revertive" switching or "fail-back" switching. In particular, Anderson teaches a network device (see FIG. 1-2, Node 103) for:

receive a failure message (see FIG. 2, 5, receiving OAM with (LOS, LOF); see col. 4, line 15 to col. 5, line 30);

re-routing traffic from the primary path to an alternate path (see FIG. 2, 3, 6, switch the traffic from working VPG to protection VPG; see col. 4, line 15 to col. 5, line 30);

allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region (see FIG. 1, Node 103 reverts the traffic from protecting VPG to working VPG when the working VPG defect/failure is cleared along in the input/ingress area/region of the working VPG (e.g. between node 101 and 102); see col. 4, line 50 to col. 5, line 15).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide “means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region” as taught by Anderson in the system of Dantu, so that it would provide extremely fast protection switching of an extremely large number of ATM virtual connections; see Anderson col. 2, line 15-20.

Regarding Claim 25, 27 and 28, Dantu discloses a network device (see FIG. 3, node 300/340/344/348; see FIG. 4-5, node 400/500; or see FIG. 6, Node 600/616/620/624) for:

detecting (see FIG. 4, a combined system of processor 402, memory 404, and interface 412 performing examining/detecting; see col. 9, line 30 to col. 11, line 26; or see FIG. 5, a combined system of processor 502, memory 504, and interface 512 performing examining/detecting; see col. 12, line 39-64; see col. 13, line 30-40) a failure along an ingress region of a primary path (see FIG. 3, a failure along a input/ingress region/section of the working path 332 between node 344 and 348 ; or see FIG. 6, a failure along a input/ingress region/section of the working path between node 600, 616, 620; see FIG. 9, step 902; see FIG. 10, step 1002; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36), where the ingress region comprises a link associated with the source network device (see FIG. 3, input/ingress region/section comprises a path/link 332 associated with the node (e.g. Node 300); or see FIG. 6, input/ingress region/section comprises a path/link associated with the node 600; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36), and the link comprises either an outgoing link (see FIG. 3, a path/link 332 comprising a transmit link/line to Node 340 or 348; or see FIG. 6, a path/link at node 600 comprising a transmit link/line to Node 616, 624; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36;,) **or** a link between the source network device and a neighboring network device (see FIG. 3, a path/link between Node 300 and neighbor node 340/344/348; or see FIG. 3, a path/link between Node 600 and neighbor node 616, 624, 620; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36); and

re-routing traffic (see FIG. 4, a combined system of processor 402, memory 404, storage 406 performing switching to protecting path ring in node 400; see col. 9, line 30 to col. 11, line 26; or see FIG. 5, a combined system of processor 502, memory 504, and storage 506 performing switching to protecting path ring in node 500; see col. 12, line 39-64; see col. 13, line 30-40) from the primary path associated with an original IP address (see FIG. 7, IP address 712/08) to an alternate path (see FIG. 3,6, protection path 336; see FIG. 7, a label 716 with path route) which includes the device using a forwarding table that includes Internet Protocol (IP) and Multi-Protocol Label Switched (MPLS) routing information (see FIG. 3, Forwarding table 312 and/or routing table 308; see FIG. 4, a combined system of memory 404 (e.g. routing table 404 A and forwarding table 404B) and storage 406 (e.g. table formation 406A and protection switching 406B) in node 400 includes IP addresses corresponding to MPLS labels; or see FIG. 5, a combined system of memory 504 (e.g. forwarding table 504A) and storage 506 (e.g. forwarding logic 506) in node 500 includes IP addresses corresponding to MPLS labels; see FIG. 10, S 1004, see FIG. 11, S 1104,1106; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-45) while associating the original IP address to the alternate path upon detection of the failure (see FIG. 4,5; see FIG. 10, S 1006,1008,1010; see FIG. 11, S 1108; see col. 9, line 50 to col. 10, line 32; see col. 11, line 10-40; see col. 12, line 40-64; see col. 13, line 30-45; see col. 14, line 45-67; see col. 15, line 23-65; see col. 18, line 45-55; see col. 19, line 35-46; switching IP address with its corresponding new label to the protection path when detecting a failure).

Dantu does not explicitly disclose “allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region”.

However, switching back from the alternating/protection path to the primary path after the failure is recovered is well known in the art as “revertive" switching or "fail-back" switching. In particular, Anderson teaches a network device (see FIG. 1-2, Node 103) for:

detecting a failure along in ingress region of a primary path (see FIG. 2, detect a physical layer defect/failure along in the input/ingress area/region (e.g. between node 101 and 103) of the working VPG ; see col. 4, line 15 to col. 5, line 30), where the ingress region comprises a link (see FIG. 2, input/ingress area/region comprises a path/link/connection) associated with the network device (see FIG. 2, associated/related with Node 103), and the link comprises an outgoing link (see FIG. 2, link/path/connection comprising outgoing/transmit link/line/connection of node 101) **or** a link between the network device and a neighboring network device (see FIG. 2, 3, link/path/connection between Node 103 and Node 101; see col. 4, line 15 to col. 5, line 30);

re-routing traffic from the primary path to an alternate path (see FIG. 2, 3, switch the traffic from working VPG to protection VPG; see col. 4, line 15 to col. 5, line 30);

allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region (see FIG. 1, Node 103 reverts the traffic from protecting VPG to working VPG when the working VPG defect/failure is cleared along in the input/ingress area/region of the working VPG (e.g. between node 101 and 103); see col. 4, line 50 to col. 5, line 15).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide "means for allowing traffic to travel along the primary path when the failure is no longer detected along the ingress region" as taught by Anderson in the system of Dantu, so that it would provide extremely fast protection switching of an extremely large number of ATM virtual connections; see Anderson col. 2, line 15-20.

Regarding Claims 3,7, 11, 15, 19, 23, 26 and 29, Dantu discloses the device is a multi-protocol label switched (MPLS) device (see FIG. 3, Node 300 with MPSL switching capability; or see FIG. 6, 7, MPLS label switch Node 600; see col. 9, line 30-36; see col. 13, line 30-35; see col. 14, line 50-65; see col. 15, line 45-65) and the primary and alternate paths are label switched paths (LSPs) (see FIG. 1, working and protection paths are label Switch Paths; see col. 9, line 30-36; see col. 13, line 30-35; see col. 14, line 50-65; see col. 15, line 45-65).

Regarding Claims 4, 12 and 20, Dantu discloses the failure is at a neighboring device (see FIG. 3, a failure occurs at neighbor node 344/348; or see FIG. 6, a failure occurs at neighbor node 616,620,622) **or** along a link between the device and the neighboring network device (see FIG. 3, failure occurs between node 300 and node 344; or see FIG. 3, failure occurs between node 600 and node 616/620; see col. 9, line 30, line 63; see col. 17, line 10-20,45-55; see col. 10, line 25-36).

Regarding Claims 8, 16, and 24, Dantu discloses the quality of service is associated with bandwidth (see col. 16, line 1-36; see col. 19, line 35-46; QoS associated with bandwith or throughput or resources).

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to IAN N. MOORE whose telephone number is (571)272-3085. The examiner can normally be reached on 9:00 AM- 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Trost can be reached on 571-272-7872. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ian N. Moore
Primary Examiner
Art Unit 2416

/Ian N. Moore/
Primary Examiner, Art Unit 2416